GAVIN NEWSOM
GOVERNOR

NANCY WARD
DIRECTOR

FISCAL YEAR 2024-25
STATE & LOCAL CYBERSECURITY GRANT – STATE AGENCY (SG)
COMPETITIVE FUNDING OPPORTUNITY
Release Date: July 31, 2024

The California Governor's Office of Emergency Services (Cal OES), Homeland Security & Emergency Management (HSEM) Branch, has a Competitive Funding Opportunity (CFO) for the (SG) Program.

This CFO provides programmatic information and the requirements necessary to prepare a proposal for Cal OES grant funds. The provisions of this CFO supersede previous RFPs. If any language in this CFO conflicts with the terms and conditions of the applicable grant program guidance (e.g., federal Notice of Funding Opportunity, California State Supplement, etc.), the grant program guidance document(s) prevail. Applicants are strongly encouraged to review the applicable Notices of Funding Opportunity and California State Supplement, which outlines the requirements that apply to Cal OES HSEM Branch Grant Subawards.

PUBLIC RECORDS ACT NOTICE

Proposals are subject to the Public Records Act, Government Code Section 7920.000, *et seq*. Do not put any personally identifiable information or private information on this proposal. If you believe that any of the information you are putting on this proposal is exempt from the Public Records Act, please indicate what portions of the proposal and the basis for the exemption. Your statement that the information is not subject to the Public Records Act will not guarantee that the information will not be disclosed.

CONTACT INFORMATION

Questions concerning this CFO or the proposal process must be submitted by email to:

State & Local Projects Unit
StateLocalProjects@caloes.ca.gov

Cal OES staff cannot assist the Applicant with the actual preparation of their proposal. Cal OES can only respond to technical questions about the CFO during the period between the publication date and completion of the CFO process.

A. ELIGIBILITY

1. Eligibility to Compete for Funding

For a proposal to be eligible to compete for funding (i.e., read and rated) all the following conditions must be met:

- Applicants must be agencies of the State of California.
- The proposal must be emailed to StateLocalProjects@caloes.ca.gov and received no later than **11:59 PM (PDT) on Friday, September 27, 2024**. Proposals must be attached as PDF documents and contain the form(s) outlined E. Proposal Requirements. **The proposal PDF file name should include "FY2024 SG Program CFO" and the Applicant entity name**. Cal OES cannot access proposals through cloud-based storage services (e.g., Google Drive, Dropbox, etc.). Emails should identify the name of the CFO in the Subject line. **If you have not received a confirmation that your proposal was received within two business days of the date it was submitted, please send an email to** StateLocalProjects@caloes.ca.gov .

Please Note: proposals that do not meet the above requirements will be disqualified (i.e., ineligible) and not read and rated.

2. Eligibility for Funding Consideration

Only one proposal per Applicant will be eligible to receive funding. If an Applicant submits more than one proposal, only the highest scoring proposal, meeting the criteria above, will be considered for funding.

3. Prerequisites to Receive Funding

If selected, all the following must be completed within 60 days of receiving the Intent to Fund notification to be eligible to receive funding, Applicants must:

- Have a Unique Entity Identifier (Unique Entity ID) registered in the federal System for Award Management (SAM). Applicants who do not currently have a Unique Entity ID will need to register at SAM.gov to obtain one. **Applicants should start this process**

immediately to ensure they are able to comply with the requirement to have this completed within the 60-days.

- **Not** have an exclusion record in the SAM by the beginning of the Program Grant Subaward performance period. An exclusion record in the SAM indicates that a contractor (agency) is listed in the (federal) government-wide system for debarment and suspension. An agency that is debarred or suspended is excluded from activities involving federal financial and nonfinancial assistance and benefits. Check SAM status.

B. FUNDING INFORMATION

There is $3,578,443 available for the Program for the Grant Subaward performance period of December 1, 2024 – December 31, 2026.

1. Funding Amount

Applicants may apply for up to $250,000 for the 25-month Grant Subaward performance period.

Please see the chart below for a sample breakdown of the fund sources (by Cal OES fund source code) and match based on the maximum request amount.

2022 SLCGP	2022 SLCGP MATCH (WAIVED)	2023 SLCGP	2023 SLCGP MATCH (WAIVED)	TOTAL PROJECT COST
$82,500	$0	$167,500	$0	$250,000

2. Funding Source(s)

Guidance on policies and procedures for managing HSEM Branch Grant Subawards funded through federal fund sources can be found in the FEMA Preparedness Grants Manual. Applicants are **strongly encouraged** to review and retain a copy of this document to familiarize themselves with program-specific information as well as overall guidance on the rules and regulations for all fund sources that support this Program.

The Program is supported through the following fund:

State & Local Cybersecurity Grant Program (SLCG)

- Provides state/territorial, local, and tribal (SLT) governments with resources to address cybersecurity risks and threats to information systems, improve the security of critical infrastructure and resilience of the services provided by those entities.

- Supports efforts to implement cyber governance and planning, assess and evaluate systems and capabilities, mitigate prioritized issues, and build a cybersecurity workforce.

- Requires Recipients and Subrecipients to participate in the federal Cybersecurity & Infrastructure Security Agency (CISA) Cyber Hygiene Service – Vulnerability Scanning and participate in the Nationwide Cybersecurity Review (NCSR) as described in the federal Notice of Funding Opportunity (NOFO).

- **For FY 2022 and FY 2023 SLCGP funding, the match requirement has been waived for all Subrecipients**. Applicants are referred to Title 2, Code of Federal Regulations (C.F.R.), Part 200, § 200.306 for additional information.

- Cal OES's fund source code for this federal fund is SLCG.

FEMA has identified the allowable categories of cost under the SLCGP Program as follows:

- Planning – Planning costs are allowable under this Program. SLCGP funds may be used for a range of planning activities, such as those associated with the development, review, and revision of holistic, entity-wide cybersecurity plans and other planning activities that support the Program goals and objectives.

- Organization – Organizational costs are allowable under this Program. SLCGP funds may be used for cybersecurity program management, development of whole community partnerships that support cybersecurity program governance, structures and mechanisms for information sharing between the public and private sector, and operational support, including ensuring

continuity of operations for essential functions.

Personnel hiring, overtime, and backfill expenses are permitted under this Program to perform allowable SLCGP planning, organization, training, exercise, and equipment activities. Personnel expenses may include, but are not limited to, training and exercise coordinators, program managers and planners, and cybersecurity navigators. The Subrecipient must demonstrate that the personnel will be sustainable.

- Equipment – Equipment costs are allowable under this Program. Unless otherwise stated, equipment must meet all applicable statutory, regulatory, and/or DHS-adopted standards to be eligible for purchase using SLCGP funds. Subrecipients will be responsible for obtaining and maintaining all necessary certifications and licenses for the requested equipment.

  Investments in emergency communications systems and equipment must meet applicable SAFECOM Guidance recommendations; such investments must be coordinated with the Statewide Interoperability Coordinator and the State Interoperability Governing Body to ensure interoperability and long-term capability.

  SLCGP funds may be used to purchase maintenance contracts or agreements, warranty coverage, licenses, and user fees in support of a system or equipment. Applicants should reference the FY 2022 and FY 2023 SLCGP NOFO, Section D, 12 – Funding Restrictions and Allowable Costs, e. Other Direct Costs, III. Equipment, for additional requirements and restrictions on allowable equipment costs, when building their Budget Detail table for their NOI.

- Training – Training costs are allowable under this Program. Allowable training-related costs under SLCGP include the establishment, support, conduct, and attendance of training and/or in conjunction with training by other federal agencies. Training conducted using SLCGP funds should align with the California SLCGP Cybersecurity Plan and address a performance gap identified through cybersecurity assessments and contribute to building a capability that will be evaluated through a formal

exercise.

Subrecipients are encouraged to use existing training, such as FEMA's National Preparedness Course Catalog, rather than developing new courses.

All training courses must receive a Training Feedback Number from Cal OES Training & Exercise prior to the start of the course. To request a Training Feedback Number, please download and complete the Training Feedback Form and forward the completed request via email to training@caloes.ca.gov .

- Exercise – Exercise costs are allowable under this Program. Exercises conducted with SLCGP funding should be managed and conducted consistent with Homeland Security Exercise and Evaluation Program (HSEEP) guidance documents.

  Subrecipients are required to submit an After Action Report/Improvement Plan (AAR/IP) to the SLCGP Grants Analyst and FEMA at hseep@fema.dhs.gov no later than 90 days after completion of any exercise(s) conducted using SLCGP funds.

- Management and Administration (M&A) – M&A costs are allowable under this Program. M&A activities are defined as directly relating to the management and administration of SLCGP subaward funds, such as financial management, reporting, and program and financial monitoring. See the FEMA Preparedness Grants Manual for examples of some M&A costs.

  Subrecipients are allowed a maximum of five (5) percent of the Grant Subaward amount for the FY 2024 SLCGP.

- Indirect Costs – Indirect costs are allowable under SLCGP; see the Indirect Costs section of the FY 2024 SLCGP State Supplement for additional guidance on including indirect costs in the budget for SLCGP-funded projects.

Applicants should select the appropriate budget categories for the costs included in their project proposal on the Notice of Interest form; see E. Programmatic Narrative, below.

In addition, the following costs are **unallowable** under the SLCGP:

- Supplantation of state or local funds.

  This shall not be construed to prohibit the use of funds under this Program for otherwise permissible uses on the basis that the Subrecipient has previously used state, local, and/or tribal government funds to support the same or similar uses.

- Any Subrecipient cost-sharing contribution, when required.
- To pay a ransom from cyberattacks.
- Spyware.
- Recreational or social purposes, or for any purpose that does not address cybersecurity risks or cybersecurity threats on information systems owned or operated by, or on behalf of, the Subrecipient entity.
- Suing the federal government or any other government entity.
- Lobbying or intervention in federal regulatory or adjudicatory proceedings.
- Acquiring land or constructing, remodeling, or altering buildings or other physical facilities.
- Cybersecurity insurance premiums.

Please refer to Title 2, C.F.R., Part 200, Subpart E – Cost Provisions, for additional guidance on allowable and unallowable costs.

C. PROGRAMMATIC INFORMATION

1. Program Overview & Objectives

The purpose of the FY 2024 SLCGP State Agency Program is to assist California state agencies address cybersecurity risks and threats to information systems, improve security of critical infrastructure and resilience of the services these entities provide to communities throughout the State of California.

Through the Infrastructure Investment and Jobs Act (IIJA) of 2021, Congress established the State and Local Cybersecurity Improvement Act, which created the State and Local Cybersecurity Grant Program and appropriated funds to be awarded to eligible state and territorial administrative agencies over a period of four federal fiscal years.

Each year, beginning with federal fiscal year 2022 through federal fiscal year 2025, the U.S. Department of Homeland Security (DHS)/Federal Emergency Management Agency (FEMA) announces a NOFO for the SLCGP. The funds provided by this Program assist SLT governments to manage and reduce systemic cyber risks, including through the establishment of a strong foundation to build a sustainable cybersecurity program. **Grant funds are intended to supplement existing fiscal resources and are not guaranteed long-term sustainability solutions.** Projects funded under this Program are expected to be reasonably sustained after the end of the performance period without the expectation to receive future grant funds.

As the SAA for this Program, Cal OES established a subcommittee of the California Cybersecurity Task Force, called the Cybersecurity Investment Planning Subcommittee (CCTF-CIPS), in order to meet specified requirements under the IIJA and SLCGP NOFO, including the development and submission of a statewide cybersecurity plan, which was submitted by Cal OES and approved by CISA on September 29, 2023. The CCTF-CIPS serves as California's cybersecurity planning committee for the purposes of the SLCGP and participates in Program activities such as updating the cybersecurity plan and developing strategies for allocating funds available through the SLCGP to projects that align with the approved cybersecurity plan.

SLCGP provides funding to implement projects that address one or more of the following objectives established by CISA to accomplish the overarching goal of the Program:

Objective 1 – Governance and Planning – Develop and establish appropriate governance structures, as well as plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.

Objective 2 – Assessment and Evaluation – Identify areas for improvement in SLT cybersecurity posture based on continuous testing, evaluation, and structured assessments.

Objective 3 – Mitigation – Implement security protections commensurate with risk (outcomes of Objectives 1 and 2), using the best practices as described in element 5 of the required 16 elements of the cybersecurity plans listed in the IIJA and those further listed on page 14 of the NOFO.

Objective 4 – Workforce Development – Ensure organization personnel are appropriately trained in cybersecurity, commensurate with their responsibilities as suggested in the National Initiative for Cybersecurity Education.

2. Program Priorities & Requirements

All proposed projects must support activities that effectively contribute to the state government agency's capability to prevent, prepare for, mitigate against, respond to, and recover from cyber threats against information systems owned and/or operated by the state government agency, align with the objectives, priorities, and cybersecurity plan elements described in the California SLCGP Cybersecurity Plan, and meet the criteria listed in the FY 2022 and FY 2023 SLCGP NOFOs.

a. SLCGP National Priorities

In developing projects for the FY 2024 SLCGP State Agency Program, Applicants should describe projects that address areas for improvement identified by the state government agency using the whole community approach as they relate to cybersecurity capabilities and especially projects that address implementation of one or more of the key Cybersecurity Best Practices, as appropriate to their organization:

- Implement multi-factor authentication.
- Implement enhanced logging.
- Data encryption for data at rest and in transit.

- End use of unsupported/end of life software and hardware that are accessible from the internet.
- Prohibit use of known/fixed/default passwords and credentials.
- Ensure ability to reconstitute systems (backups).
- Actively engage in bidirectional sharing between CISA and SLT entities in cyber relevant time frames to drive down cyber risk.
- Migration to the .gov internet domain.

Educational institution Subrecipients (e.g., school districts) using the .edu Internet domain are exempted from transitioning to the .gov Internet domain. All other Subrecipients of SLCGP funding are highly encouraged to transition to a .gov Internet domain over time. Additional information on migrating to the .gov Internet domain can be found on the DotGov Program website.

DHS/FEMA does not prescribe a minimum funding amount for these priorities. However, all SLCGP Applicants are encouraged to consider how FY 2024 SLCGP State Agency Program funding can be used to support these priority areas as they apply to the state government agency's specific needs and the needs of the whole community. Subrecipients of funding through SLCGP are strongly encouraged to eventually adopt and use all eight of the Cybersecurity Best Practices listed above.

Additional information about these cybersecurity best practices can be found in the FY 2022 and FY 2023 SLCGP NOFOs, Section A, 10, c.

b. SLCGP Statewide Priorities

The CCTF-CIPS, in its SLCGP Cybersecurity Plan, described an intention to focus on the following initiatives, with the corresponding cybersecurity plan element from the IIJA noted in parentheses, to strengthen cybersecurity across California using the FY 2022-23 SLCGP funds:

- Enhance the preparation, response, and resiliency of information systems, applications, and user accounts (Element 3);
- Implement a process of continuous cybersecurity risk factors and threat mitigation practices prioritized by degree of risk (Element 4);
- Develop and coordinate strategies to address cybersecurity risks and threats (Element 14);
- Identify and mitigate any gaps in the cybersecurity workforce, enhance recruitment and retention efforts, and bolster the knowledge, skills, and abilities of personnel with reference to the National Initiative for Cybersecurity Education – Workforce Framework for Cybersecurity (Element 8);
- Assess and mitigate Critical Infrastructure and Key Resources risks and threats impacting local jurisdictions (Element 10);
- Ensure continuity of operations including by conducting exercises (Element 7); and
- Ensure rural communities have adequate access to, and participation in, plan activities (Element 15).

SLCGP Applicants are strongly encouraged to incorporate one or more of these statewide priorities in their project description for the project(s) proposed using Program funds. **Additional information about the cybersecurity plan elements is available in the FY 2022 SLCGP NOFO, Appendix C: Cybersecurity Plan, Required Elements**.

c. Participation in Required Cybersecurity Services

Subrecipients are required to participate in free Cyber Hygiene Services – Vulnerability Scanning, provided by CISA. For these required services, please note that participation is not required to submit a proposal under this RFP but is a post-award requirement for all projects selected to receive SLCGP funding.

Additional information on this and other, optional but encouraged cybersecurity services, memberships, and resources can be found on the CISA - SLCGP website (scroll down to the Tools and Resources section).

d. Nationwide Cybersecurity Review (NCSR)

The NCSR is a free, anonymous, annual self-assessment designed to measure gaps and capabilities of a SLT's cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework and is sponsored by DHS and the Multi-State Information Sharing and Analysis Center.

SLCGP Subrecipients are required to complete the NCSR during the first year of the Grant Subaward performance period and annually thereafter until closeout. The open assessment period is usually October through February; Subrecipients may contact their assigned SLCGP Grants Analyst for additional information and technical support.

D. PROGRAM REPORTING REQUIREMENTS

Performance and implementation reports serve as a record for the implementation of the Grant Subaward. Statistics for performance and implementation reports should be collected on a quarterly basis, even when reporting occurs less frequently. The following reports are required:

a. FEMA Reports

There is one FEMA report Subrecipients will need to complete:

Annual Performance Progress Reports (PPR)

Subrecipients must submit PPR to Cal OES annually until all grant activities are completed and the Grant Subaward is formally closed out. PPR are due within 30 days after the end of the reporting period. Annual PPR must include progress made on approved activities and any other project-specific information required by Cal OES. PPR are cumulative and each annual report will include information provided by the Subrecipient in previous reporting periods.

In order to ensure that mandated performance metrics and other data required by the Grant Subaward are reported accurately, SLCGP PPR must first be submitted via email to the Cal OES SLCGP Grants Analyst for review. Electronic reports should be submitted to Cal OES for review at least seven (7) calendar days before the due date. Submission of the final, signed electronic report should only occur after the Subrecipient is instructed by the Grants Analyst to do so.

There are two annual PPR required for the Program. Failure to submit a PPR could result in Grant Subaward reduction, suspension, or termination. See the chart below for report periods and due dates.

Report	Report Period	Due Date
1st Report	December 1, 2024 – November 30, 2025	December 31, 2025
Final Report	December 1, 2025 – December 31, 2026	January 31, 2027

*Exact dates will be provided by your Grants Analyst at the end of each quarter.

E. PROGRAMMATIC NARRATIVE

Applicants must use the forms provided on the Cal OES website. **Applicants may not alter the formatting of any forms, including the Notice of Interest (NOI).** If a space or character limitation is specified under each NOI question, strict adherence to the space limitation is required. **Information included beyond the space limitation and/or unrequested attachments will not be considered in the rating process**.

Applicants must respond to each question in the NOI form. The Applicant's response to each question will be evaluated as part of the rating process. Applicants should develop a thorough project proposal that takes into consideration planning and implementation of the entire process for the proposed project from conception to completion of all activities using the requested funding.

Proposals must be aligned to one or more of the SLCGP Objectives and at least one of the 16 Cybersecurity Plan Elements. This alignment is based on how many and to what degree the associated elements are adopted, especially the eight best practices listed above (see California Cybersecurity Plan, Appendix B: Project Summary Worksheet, Related Required Element # column).

Applicants should also consider the Program priorities and requirements referenced above in C, Programmatic Information, as well as the SLCGP FY 2022 NOFO, FY 2023 NOFO and the SLCGP California State Supplement, when developing their project proposals.

In addition to their responses on the NOI form, Applicants must complete an online Cybersecurity Maturity Survey (not scored). **Upon completion of the survey, Applicants must download a copy of their survey responses and attach as a PDF file to submit with their proposal; proposals submitted without completing the survey may not be considered for funding.**

F. SELECTION OF PROPOSAL FOR FUNDING

1. Proposal Rating

Eligible proposals submitted via email as specified in A. Eligibility, above, by the due date are generally evaluated by a three-member team. Each question is assigned a point value and the Applicant's response to each question is evaluated on the following criteria:

ABSENT: The response does not address the specific question, or a response was not provided.

UNSATISFACTORY: The response does not completely address the question. The information presented does not provide a good understanding of Applicant's intent, does not give the detailed information requested by the CFO, and/or does not adequately support the proposal or the intent of the Program.

SATISFACTORY: The response addresses the question and provides a good understanding of the Applicant's intent. The response adequately supports the proposal and the intent of the Program.

ABOVE AVERAGE: The response is above average and provides a clear and detailed understanding of the Applicant's intent. The response presents a persuasive argument that supports the proposal and the intent of the Program.

EXCELLENT: The response is outstanding, with clear, detailed, and relevant information. The response presents a compelling argument that supports the proposal and the intent of the Program.

In addition to evaluating and assigning a point value to the Applicant's responses to the Programmatic Narrative Questions, the budget table and milestones submitted on the NOI form will be evaluated and assigned a point value.

The rater scores are averaged and ranked numerically. Proposals are only evaluated numerically; no notes are taken during the evaluation.

Project proposals that do not clearly and directly address the required program objectives/investment justifications or cannot be completed within the performance period will be disqualified.

2. Funding Decision

Final funding decisions are made by the Director of Cal OES. Funding decisions are based on the following:

- The ranked score of the proposal.
- Consideration of priorities or geographical distribution specific to this CFO.
- Prior negative administrative and programmatic performance, if applicable.

Applicants previously funded by Cal OES will be reviewed for poor past compliance, including fiscal management, progress and annual reports, audit reports, and other relevant documentation or information. This review may result in one or more of the following actions:

- The Applicant may not be selected for funding.
- The amount of funding may be reduced.
- Grant Subaward Conditions may be added to the Grant Subaward.

3. Notification Process

All Applicants will be notified in writing, via electronic communication, the results of the rating process. The notification will be sent to the Authorized Agent and the Primary Point of Contact identified on the NOI submitted with the proposal.

Applicants will receive one of the following notifications:

- Intent to Fund if selected for funding.
- Denial if not selected for funding, including the Applicant's scores and information regarding the appeal process.
- Ineligibility:
    - If the proposal did not meet Eligibility to Compete for Funding including information regarding the appeal process; or
    - If the proposal scored less than the required 50% of points possible, including the Applicant's scores and information regarding the appeal process.

Cal OES can only respond to technical questions about the CFO during the period between the publication date and completion of the CFO process. Requests for records must be made through a Public Records Act request.

G. FINALIZING THE GRANT SUBAWARD

1. Grant Subaward Application

Once selected for funding, Subrecipients must complete and submit their Grant Subaward Application through the online Cal OES Grants Central System (GCS). Cal OES may require revisions and/or additional documentation to finalize the submission of the Grant Subaward Application. The Grants Analyst identified in the Subrecipient's Intent to Fund notification can provide technical assistance in completing these components.

For more information on the GCS, please see the FY 2024 SLCGP California State Supplement to the NOFO.

2. Grant Subaward Approval

The Grant Subaward will be available in the Cal OES Grants Central System. The Subrecipient is not authorized to incur costs against the Grant Subaward until the application is approved. Once the Grant Subaward is approved, a request for payment may be submitted.

a. Grant Subaward Conditions

Cal OES may add conditions to execute the Grant Subaward. If conditions are added, these will be discussed with the Subrecipient and will become part of the Grant Subaward.

Grant Subaward Conditions may include holds on funding amounts included in the budget for items of cost that require prior approval from Cal OES and/or DHS/FEMA, including but not limited to, training, and meals/beverages for training and exercise events.

b. Grant Subaward Amounts

When the amount of funds available is limited, Cal OES may reduce the amount of the Grant Subaward from the amount requested by the Subrecipient. In addition, Cal OES reserves the right to negotiate budgetary changes with the Subrecipient prior to executing the Grant Subaward. If either of these actions is required, Cal OES will notify the Subrecipient prior to executing the Grant Subaward.

3. Standard Grant Subaward Funding Authority

Allocation of funds is contingent on the enactment of the State Budget. Cal OES does not have the authority to disburse funds until the State Budget is passed, and the Grant Subaward is fully executed. Expenditures incurred prior to authorization are made at the Subrecipient's own risk and may be disallowed. Cal OES employees are not able to authorize a Subrecipient to incur expenses or financial obligations prior to the execution of a Grant Subaward. However, once the Grant Subaward is finalized the Subrecipient may claim reimbursement for expenses incurred on, or after, the start of the Grant Subaward performance period.

If, during the Grant Subaward performance period, the state and/or federal funds appropriated for the purposes of the Grant Subaward are reduced or eliminated by the California Legislature or the United States Government, or in the event revenues are not collected at the level appropriated, Cal OES may immediately terminate or reduce the Grant Subaward by written notice to the Subrecipient.

Cal OES Grant Subawards are subject to applicable restrictions, limitations, or conditions enacted by the California Legislature and/or the United States Government, after, the execution of the Grant Subaward.